Penetration Testing

A QinetiQ Cyber Security Service

Key Benefits

* Identifies how real-world attackers would compromise your systems
* Provides prioritised recommendations and guidance to fast track remediation
* Provides real actionable intelligence against your security posture
* Highly experienced Security Cleared and Developed Vetting CHECK specialists

QinetiQ's Security Health Check Penetration Testing services cover application, infrastructure, wireless, cloud and mobile environments. Our certified specialists use industry best practice and extensive experience to identify vulnerabilities in systems, the risks they pose, the consequences of their configuration, and a tailored recommendation for the issue, which makes sense for your business.

We continually adapt to new ways of working. Ransomware attacks are more prevalent and remote working is becoming the new norm. Both government and commercial organisations have recently come under sustained, and at times damaging, attack from increasingly capable adversaries.

Recent high-profile security compromises have proved that whilst the theft of intellectual property or subscriber data can have regulatory or financial implications, the reputational damage that can result from such a breach can have far reaching implications for even the biggest multinationals.

It has also shown that attackers are becoming increasingly sophisticated and are now using multidimensional attacks a gainst their targets. The security of information systems is of paramount importance to almost every type of organisation, as core business functions often depend on digital data, services and infrastructure.

Our methodologies have been extensively examined, our expertise is trusted, and our reporting standards are held in high regard, which is why we are a trusted supplier to many large and small UK government entities.

The QinetiQ Approach

QinetiQ's subject matter experts will undertake testing that aims to simulate attacks against a target application or network using the same tools and techniques as the most highly skilled adversary. Throughout this process QinetiQ experts liaise with the customer to ensure they are kept informed of progress.

All engagements are expertly managed from inception to delivery and include the generation of clear and concise reporting in a timely manner. Our reports prioritise areas of technical risk and present them in an easily understandable and actionable format.

QinetiQ can offer SC and higher cleared security specialists with both industry standard CREST, Tigerscheme and Cyber Scheme qualifications.

QinetiQ offers both on-site and remote, internet-based assessments.

in association with National Cyber Security Centre

CHECK IT Health Check Service

CREST

TIGERSCHEME Providing excellence in penetration testing

QINETIQ

Service Summary

Infrastructure Testing

This area covers the testing of servers, security devices and network components to ensure they are built and secured in line with best practice. Testing can simulate either internal or external attack, giving an organisation a view of its exposure to multiple attack groups, allowing customers to gauge whether their current security architecture gives them sufficient defence in depth.

Application Testing

Application tests assess the threat from both authenticated and unauthenticated attackers to published applications. Testing will look at many areas of potential concern including user and role separation, session management, input validation and logic errors.

Cloud Infrastructure Testing

Providing assurance that cloud-hosted infrastructure has been well configured, is operating as designed and intended, and is in line with security best practices. Findings from detailed authenticated reviews can be caveated with the ease of discovery or exploitation from the perspective of unauthenticated attackers to reveal realistic risk ratings.

Cloud Application Testing

Whether it be Microsoft's Azure, Amazon's AWS or another popular provider, QinetiQ can examine the security of an organisation's cloud-hosted web applications, whether they be traditionally hosted, Lambda or Azure functions, or in public or private clouds. Testing can be per formed from various role perspectives to provide end-to-end coverage.

Wireless Testing

QinetiQ can test networks based on both 802.11 and Bluetooth. Testing will start with an RF Site Survey which determines whether the network under test can be attack ed from outside of the property boundaries. Subsequent testing will aim to identify rogue devices and will give an assessment of whether the security of the network can be compromised by an attacker.

Internet Facing Security Posture Assessment

Examine your organisation's Internet-facing security posture from the perspective of a remote threat actor getting ready to perform a stand-off electronic targeted attack. These exercises are used by QinetiQ's clients to proactively examine the attack surface of the organisation, to exercise data loss protection ontrols, and test Intrusion detection effectiveness.

Mobile Testing

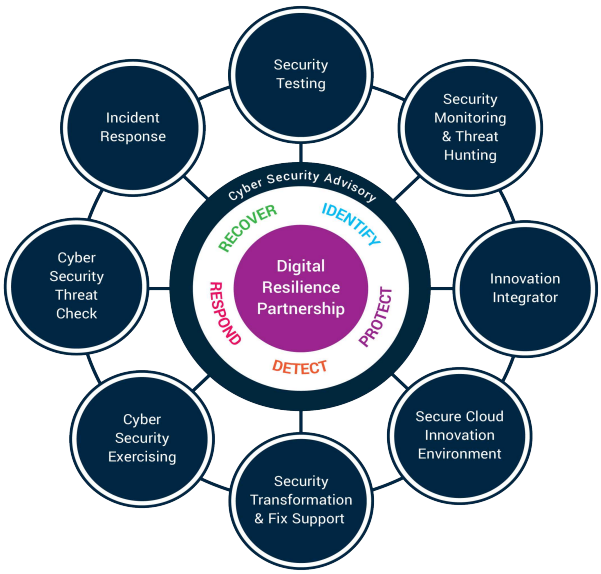
QinetiQ has undertaken numerous bespoke assessments into both existing and new hardware and software solutions. Solution providers can use the output of this testing to further increase the security of their solution, whilst customers can use the testing to inform product selection processes.

Other IT Health Check Features

- Voice Over IP (VOIP)
- On-Host Audits
- Network Vulnerability Assessment (VA)
- Active Domain Directory Review
- Server, Workstation and Laptop Build Review
- Network Device and Firewall Ruleset Review

Other QinetiQ Cyber Services

This service forms part of a wider service portfolio, which seeks to help organisations mature their digital resilience and to help build confidence in their ability to deal with cyber-attacks, through a holistic approach. his service is a sub-service of Enterprise Cyber.



Why QinetiQ Cyber

- Unmatched team of vetted, expert cyber consultants, architects, engineers and human-performance scientists
- Unique experience and patented intellectual property in securing the world's most complex, safety-critical environments
- NCSC Certified Cyber Professionals and Services

www.QinetiQ.com

For further information please contact:

Malvern Technolgy Centre
St Andrews Road
Malvern
WR14 3PS
+44(0)1252 392000

SHC@QinetiQ.com
CyberEnquiries@QinetiQ.com